

102年公務人員特種考試警察人員考試、
102年公務人員特種考試一般警察人員考試及
102年特種考試交通事業鐵路人員考試試題

代號：20160

全一頁

等 別：二等一般警察人員考試

類 科：刑事警察人員數位鑑識組

科 目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）

考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、請詳細解釋下列專有名詞：（每小題 5 分，共 20 分）

(一)旁通道攻擊（side-channel attacks）

(二)弱點掃描（vulnerability scan）

(三)共同準則（common criteria）

(四)強制型存取控制（mandatory access control）

二、位址解析協定（Address Resolution Protocol, ARP）愚弄（spoofing）（通稱 ARP spoofing）是進行中間人攻擊（man-in-the-middle attack）的常用手法，請問：

(一)何謂中間人攻擊？請舉例說明。（5 分）

(二)ARP spoofing 的工作原理為何？請詳細說明之。（10 分）

(三)DNS（domain name service）spoofing 和 ARP spoofing 有何不同？請簡述其工作原理。（5 分）

三、開發資訊系統時，如果遵循一些安全設計原則（security principles），這樣即使系統遭受攻擊，也可以降低損害。請針對下列四個安全設計原則，分別說明其意義，並舉例說明若遵照該原則，可以減少那方面的損害？（每小題 5 分，共 20 分）

(一)最小權限（least privilege）

(二)完全仲裁（complete mediation）

(三)分散權限（separation of duties）

(四)預設失效安全（fail-safe default）

四、有關防火牆（firewall）：

(一)封包過濾式防火牆（packet filtering firewall）和代理人為基底式防火牆（proxy-based firewall）的工作原理有何不同？請分別說明之。（10 分）

(二)防火牆和入侵預防系統（intrusion prevention system, IPS）有何區別？請詳細說明之。（10 分）

五、有關數位鑑識（digital forensics）：

(一)數位鑑識的目的為何？請詳細說明之。（10 分）

(二)請列出進行數位鑑識必須經歷的幾個步驟（請依先後次序列出），並簡單說明各步驟的意義。（10 分）